Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Symbolic Computation 39 (2005) 671–688

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

An algorithm for constructing representations of finite groups

Vahid Dabbaghian-Abdoly*

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, Canada K1S 5B6

Received 16 November 2003; accepted 9 January 2005
Available online 26 February 2005

Abstract

Let G be a finite group. It is easy to compute the character of G corresponding to a given complex representation, but much more difficult to compute a representation affording a given character. In part this is due to the fact that a class of equivalent representations contains no natural canonical representation.

Although there is a large literature devoted to computing representations, and methods are known for particular classes of groups, we know of no general method which has been proposed which is practical for any but small groups.

We shall describe an algorithm for computing an irreducible matrix representation $\mathcal{R}$ which affords a given character χ of a given group G. The algorithm uses properties of the structure of G which can be computed efficiently by a program such as GAP, theoretical results from representation theory, theorems from group theory (including the classification of finite simple groups), and linear algebra. All results in this paper have been implemented in the GAP package REPSN.

MSC: primary 20C40, secondary 20C15

Keywords: Algorithm; Perfect groups; Irreducible representations

* Corresponding address: Computer Science, University of Calgary, 2500 University Dr. NW, T2N 1N4 Calgary, Alberta, Canada. Tel.: +1 403 210 9544; fax: +1 403 284 4707.
E-mail address: vdabbagh@math.carleton.ca.

0747-7171/$ - see front matter
doi:10.1016/j.jsc.2005.01.002

1. Introduction

The construction of representations is a classical problem which dates back over a century. One early example appears in Burnside (1955, page 302) where an irreducible representation of degree 3 for the alternating group on five elements is constructed.

Even earlier (1878) C. Jordan constructed the primitive linear groups of degree 2 and his work was extended in Blichfeldt (1917), Brauer (1967), and Wales (1969, 1970). Using the classification of finite simple groups, Dixon and Zalesskii (1998) describes all primitive finite linear groups of prime degree.

We can divide the methods and algorithms which have been proposed for constructing representations of finite groups into two main classes: the methods which deal with the problem theoretically and the methods and algorithms which deal with it in a practical sense. So far none of them has proved effective as a method of solving the problem for more than a very limited class of groups.

There are satisfactory methods for constructing modular representations of groups over finite fields and Parker's *MEATAXE* is an effective tool for computing with modular representations (see Parker, 1984; Holt and Rees, 1994). This method is extended to the ring of integers in Parker (1998).

Some computer programs have been written for computing complex representations of finite groups (see, for example, Flodmark and Blokker, 1967; Brott and Neubüser, 1970; Gollan and Grabmeier, 1990; Müller and Clausen, 2001).

Also there have been presented some methods for constructing or approximating representations of some particular groups (see, for example, Böge, 1993; Dixon, 1970; Dixon and Gollan, 1993; Janusz, 1966; Pergler, 1995; Piatetski-Shapiro, 1983; Plesken and Souvignier, 1996, 1997, 1998).

Some theoretical methods are established in Babai and Rónyai (1990), Babai and Friedl (1991), Baum (1991), Baum and Clausen (1995), and Eberly (1989) for finding irreducible representations of a finite group G over the field of complex numbers. These methods show that the computational complexity of the problem is bounded by a polynomial in $|G|$. In our situation the input to the program is much more concise than listing the elements in the group. This suggests that from our point of view these theoretical results are not using the right measure of complexity.

Let $G = \langle S \rangle$ be a finite group and χ be an ordinary irreducible character of G. In this paper we present a method for constructing a representation $\mathcal{R}$ of G affording χ. We proceed recursively, reducing the problem to smaller subgroups of G or characters of smaller degree until we obtain a problem with which we can deal directly.

The inputs of this algorithm are a given set S of generators of G, and the character χ. The output is a list of matrices $\mathcal{R}(x)$ $(x \in S)$ corresponding to the generators of G. We will show that this algorithm works for all groups and all irreducible characters χ of degree less than 32 although in principle the same methods can be extended to characters of larger degree. This algorithm has been implemented in the `GAP` package `REPSN` (Dabbaghian-Abdoly, 2004).

There is no upper bound depending only on n for the order of a group with a faithful representation of degree n (but see Jordan's theorem (Isaacs, 1976, Theorem 14.12)).

However, in general such groups may have orders which are exponential in n. For example, S_{n+1} has a faithful representation of degree n.

Our object is to construct a program for computing a representation of a group G affording a specific character of degree n whose execution time depends principally on steps which take time bounded by a small power of n and avoid dependence on the size of G. Our program uses a number of functions from GAP whose time complexity may be difficult to estimate (such as solution of linear equations over a cyclotomic field), and the execution time of some of these functions certainly depends on the way in which G is originally presented. For example, if G is provided as a permutation group, then the execution time of some of the functions will depend on the degree of the permutations, but in general not on the size of G. In practice, we seem to have been successful, and our program REPSN is able to handle quite large groups provided the degree is not too large.

Overview: Our algorithm is recursive. Given a set of generators for a group G in a suitable form (often as permutations) and a faithful irreducible character χ we try to reduce the problem to the corresponding problem for a proper subgroup of G.

Our first series of subprograms perform this reduction in the case $G' < G$ and use induction method (Section 2.1) and Theorems 2.2 and 2.1. These subprograms do not depend on bounding the degree of χ by 32. In particular, if G is solvable, then they eventually reduce the problem to the trivial group and so complete the construction of the representation of G.

If G is not solvable then the problem is recursively reduced to the case where $G = G'$, so G is a perfect group. It is only in this situation that we require the character to have degree <32. When G is perfect, G will either have a normal abelian subgroup $A \not\leq Z(G)$, or $Z(G)$ is the unique maximal normal subgroup of G. In the former case χ is imprimitive and recursion can be used again (see Section 4.3). In the latter case, we know that G can be written as a central product by Corollary 3.5. If there is more than one factor in this central product then Theorem 3.4 applies and we can recursively reduce to a smaller group.

If there is only one factor in this central product, then either G is a central cover of a non-abelian simple group or G is a perfect group such that $\mathrm{Soc}(G/Z(G))$ is abelian. We deal with these two cases in Section 4.2 (using the character restriction method) and in Section 4.3 (using ad hoc methods).

In implementing this algorithm as RESPN we use a number of GAP functions. These include: computing generators for subgroups, finding the derived series for a group, finding minimal normal subgroups, and character calculations such as computing constituents of a character. In particular, it is necessary to compute the irreducible characters for some of the subgroups involved in order to carry out the reduction of χ restricted to that subgroup.

2. Reduction to perfect groups

In this section we introduce the methods of induction and extension and then explain how the methods of induction and extension enable us to reduce our problem to the case where G is perfect. The case where G is perfect is dealt with using the tensor product construction and the character restriction method.

2.1. Induction

Let χ be an irreducible character of a finite group G. If N is a normal subgroup of G then using Clifford's Theorem we have

$$\chi_N = e \sum_{i=1}^{t} \theta_i$$

where $\theta = \theta_1, \ldots, \theta_t$ are the distinct conjugates of an irreducible character θ of N and e is an integer $\geqslant 1$.

If we consider $T := \mathrm{I}_G(\theta)$, the inertia subgroup of θ in G, then $t = |G : T|$. It is shown in Isaacs (1976, Theorem 6.11) that there exists an irreducible character ψ of T such that $\psi_N = e\theta$ and $\psi^G = \chi$.

If $t > 1$, then T is a proper subgroup of G, and from a representation of T affording ψ we can construct an induced representation of G affording $\psi^G = \chi$. Let $l_1, \ldots, l_t$ be a left transversal of T in G. If $\mathcal{R}$ is a representation of T affording ψ then $\mathcal{R}^G(g) = [\breve{\mathcal{R}}(l_i^{-1} g l_j)]$ is the induced representation of G affording χ where $g \in G$ and

$$\breve{\mathcal{R}}(x) = \begin{cases} \mathcal{R}(x) & \text{if } x \in T \\ 0 & \text{if } x \notin T. \end{cases}$$

This will enable us in many cases to reduce our problem of finding a representation affording χ to one of finding a representation affording a character on a proper subgroup.

2.2. Extension

Theorem 2.1. *Let $H = \langle a_1, \ldots, a_m \rangle$ be a normal subgroup of a group G and χ be an irreducible character of degree n of G such that χ_H is irreducible. Let $\mathcal{R}_0$ be a representation of H affording χ_H. Suppose $z \in G \backslash H$ and $\chi(z) \neq 0$. If a representation $\mathcal{R}$ of G affording χ is the extension of $\mathcal{R}_0$, then $\mathcal{R}_0(a_t)\mathcal{R}(z) = \mathcal{R}(z)\mathcal{R}_0(b_t)$ where $b_t = z^{-1} a_t z \in H$ and $t = 1, \ldots, m$. Let $\mathcal{R}(z) = [z_{ij}]$, $\mathcal{R}_0(a_t) = [a^t_{ij}]$ and $\mathcal{R}_0(b_t) = [b^t_{ij}]$. Then the system of $mn^2 + 1$ equations*

$$\sum_{k=1}^{n} (a^t_{ik} z_{kj} - z_{ik} b^t_{kj}) = 0 \qquad \textit{for} \qquad 0 \leqslant i, j \leqslant n, \quad t = 1, \ldots, m \tag{1}$$

and

$$\mathrm{tr}([z_{ij}]) = \chi(z) \tag{2}$$

has a unique solution which determines the entries of $\mathcal{R}(z)$.

Proof. We first show that there exists a representation $\mathcal{R}$ of G which affords χ and $\mathcal{R}_H = \mathcal{R}_0$. Indeed, let $\mathcal{S}$ be any representation of G affording χ. Then $\mathcal{S}_H$ affords χ_H and so is equivalent to $\mathcal{R}_0$. Hence there exists an invertible matrix C such that $C^{-1}\mathcal{S}(x)C = \mathcal{R}_0(x)$ for all $x \in H$. Now $\mathcal{R}$ defined by $\mathcal{R}(z) = C^{-1}\mathcal{S}(z)C$ for all $z \in G$ clearly satisfies the required conditions.

We next show that the Eqs. (1) and (2) determine $\mathcal{R}(z) = [z_{ij}]$ completely when $\chi(z) \neq 0$. Indeed, suppose $W = [w_{ij}]$ is an $n \times n$ matrix whose entries satisfy (1) and (2).

Then Eq. (1) shows that $\mathcal{R}_0(a_t)W = W\mathcal{R}_0(b_t)$ for $t = 1, \ldots, m$. Since $H = \langle a_1, \ldots, a_m \rangle$, we conclude that $W\mathcal{R}(z)^{-1}$ commutes with all $\mathcal{R}_0(x)$ $(x \in H)$. Because $\mathcal{R}_0$ is irreducible, Schur's lemma now shows that $W\mathcal{R}(z)^{-1} = \lambda I$ for some scalar λ. Now (2) shows that $\chi(x) = \operatorname{tr} W = \operatorname{tr} \lambda\mathcal{R}(z) = \lambda\chi(z)$. Since $\chi(z) \neq 0$ this implies that $\lambda = 1$ and so $W = \mathcal{R}(z)$ as claimed. □

The condition $\chi(z) \neq 0$ in the theorem is easily satisfied. Indeed, Theorem 2.2 below shows that if $\chi(z) = 0$, then $\chi(zw) \neq 0$ for some $w \in N$.

Extending a representation using Theorem 2.1 requires solution of a system of (consistent) linear equations in n^2 unknowns. The time taken to carry this out is known to be asymptotic to cn^6 where c measures the time for carrying out a multiplication or division of two scalars. This is often a bottleneck in the execution of our program especially when the coefficients lie outside of $\mathbb{Q}$. In the latter case GAP deals with the coefficients as cyclotomic expressions and this slows down the computation.

It is also possible to extend an irreducible representation in a similar way from subgroups which are not normal, as Theorem 2.2 will show. The computations are more complicated, and fortunately we do not require this case very often.

Theorem 2.2. *Let G be a group with an irreducible character χ of degree n and H be a subgroup of G such that χ_H is irreducible. Let $\mathcal{R}_0$ be a representation of H affording χ_H. By a theorem of Burnside there exist $w_1, \ldots, w_{n^2} \in H$ such that $\mathcal{B} = \{\mathcal{R}_0(w_1), \ldots, \mathcal{R}_0(w_{n^2})\}$ is a basis for the full matrix algebra $M_{n\times n}$. Then $\mathcal{R}_0$ can be extended uniquely to a representation $\mathcal{R}$ of G affording χ and the entries of $\mathcal{R}(z)$ for $z \in G$ are determined by the equations*

$$\chi(w_k z) = \operatorname{tr}(\mathcal{R}_0(w_k)\mathcal{R}(z)) \qquad \textit{for } k = 1, \ldots, n^2.$$

Proof. Let $\mathcal{R}$ be a representation affording χ and extending $\mathcal{R}_0$. We find the entries of $\mathcal{R}(z) := [z_{ij}]$ for $z \in G$. Suppose $\mathcal{S} = \{E_{ij} \mid 1 \leqslant i, j \leqslant n\}$ is the standard basis of $M_{n\times n}$, where the entries of E_{ij} are 1 at position (i, j) and 0 elsewhere. Since $\mathcal{B}$ is a basis for $M_{n\times n}$, for each $1 \leqslant i, j \leqslant n$ we have

$$E_{ij} = \sum_{k=1}^{n^2} \alpha_{ijk}\mathcal{R}_0(w_k) \qquad \text{for some } \alpha_{ijk} \in \mathbb{C}$$

where the α_{ijk} are unique. Since

$$\chi(w_k z) = \operatorname{tr}\mathcal{R}(w_k z) = \operatorname{tr}(\mathcal{R}_0(w_k)\mathcal{R}(z))$$

we have

$$\begin{aligned}\sum_{k=1}^{n^2} \alpha_{ijk}\chi(w_k z) &= \sum_{k=1}^{n^2} \alpha_{ijk}\operatorname{tr}(\mathcal{R}_0(w_k)\mathcal{R}(z)) \\ &= \operatorname{tr}\left(\sum_{k=1}^{n^2} \alpha_{ijk}\mathcal{R}_0(w_k)\mathcal{R}(z)\right) = \operatorname{tr}(E_{ij}\mathcal{R}(z)).\end{aligned}$$

However $\mathrm{tr}(E_{ij}\mathcal{R}(z)) = z_{ji}$ so

$$z_{ji} = \sum_{k=1}^{n^2} \alpha_{ijk}\chi(w_k z) \qquad \text{for } 1 \leqslant i, j \leqslant n.$$

This completes the proof. $\square$

In order to apply Theorem 2.2 it is necessary to construct a suitable basis $\mathcal{B}$. This can be done using a probabilistic algorithm. The following theorem shows that on average at most $2n^2$ random selection of elements of H are enough to yield the basis $\mathcal{B}$.

Theorem 2.3. *Let $H = \langle T \rangle$ be a group where $T = \{t_1, \ldots, t_n\}$ and let V be an irreducible H-module. Suppose U is a proper subspace of V. Put $X = \{t_1^{\epsilon_1} \ldots t_n^{\epsilon_n} \mid \epsilon_i = 0$ or 1 for $1 \leqslant i \leqslant n\}$. As the ϵ_i take values 0 or 1 at random, the probability that $Ux \neq U$ for $x \in X$ is at least $1/2$.*

Proof (*Compare with Cooperman and Finkelstein (1993, Prop 2.1)*). For $h \in H$ we say h has $\mathcal{P}$ if $Uh \neq U$. At least one t_i has $\mathcal{P}$ since otherwise $Uh = U$ for all $h \in H$ contrary to hypothesis. Now every element of X has the form

$$x = \overbrace{t_1^{\epsilon_1} \ldots t_{k-1}^{\epsilon_{k-1}}}^{y}\, t_k^{\epsilon_k}\, \overbrace{t_{k+1}^{\epsilon_{k+1}} \ldots t_n^{\epsilon_n}}^{z}$$

where k is the largest i such that t_i has $\mathcal{P}$.

To prove the theorem it is enough to show that for fixed y and z at least one of yt_kz or yz has $\mathcal{P}$. Indeed $Uz = U$ by the choice of k. Hence if $Uyz = U$ then $Uy = U$. But then $Uyt_k = Ut_k \neq U$ and so yt_kz has $\mathcal{P}$ as required. $\square$

Minkwitz (1996) proposed another method for extending a representation affording χ_H of H to G, when the character χ_H is irreducible. His method requires a loop over the set of all elements of the subgroup H. Thus this method appears to be limited to cases where the subgroup H is fairly small (see Section 5). We have not used his method since we are looking for execution times which depend principally on the degree n of the character and not on the size of the groups involved.

2.3. Reduction to $G^{(\infty)}$

If G is not perfect then we can reduce our problem to constructing a representation for a proper subgroup using induction and extension methods.

Suppose

$$G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(\infty)}$$

is the derived series of G. If G is solvable then $G^{(\infty)} = 1$; otherwise $G^{(\infty)}$ is a non-trivial perfect subgroup of G. Since each $G^{(i)}$ is normal in G, for each $i \geqslant 1$ we have

$$\chi_{G^{(i)}} = e_i \sum_{j=1}^{t_i} \theta_{ij} \tag{3}$$

where $\theta_i = \theta_{i1}, \ldots, \theta_{it_i}$ are the distinct G-conjugates of the irreducible character θ_i of $G^{(i)}$. Now we consider three different possibilities for the values of t_i and e_i in (3) for $i \geqslant 1$.

Case I. At least one $t_i > 1$.

Put $\theta := \theta_{i1}$ and $T := \mathrm{I}_G(\theta)$, so $G^{(i)} \leqslant T < G$ and $|G : T| = t_i$. Then there exists an irreducible character ψ of T such that $\psi_{G^{(i)}} = e_i\theta$ and $\psi^G = \chi$. Hence if $\mathcal{R}$ is a representation of T affording ψ then $\mathcal{R}^G$ is a representation of G affording χ.

Case II. All $t_i = 1$ and $e_1 > 1$.

Let

$$G = K_0 \rhd K_1 \rhd \cdots \rhd K_m = G^{(1)}$$

be a composition series of G through $G^{(1)}$. Then for $1 \leqslant u \leqslant m$, $|K_{u-1} : K_u|$ is a prime and K_u is a normal subgroup of G. Since $t_1 = 1$ and $e_1 > 1$, $\chi_{G^{(1)}}$ is reducible. This means there exists $1 \leqslant u \leqslant m$ such that $\chi_{K_{u-1}}$ is irreducible and χ_{K_u} is reducible. Since $|K_{u-1} : K_u| = p$ is a prime and K_u is normal in G, Isaacs (1976, Corollary 6.19) shows that

$$\chi_{K_u} = \sum_{j=1}^{p} \varphi_j$$

where $\varphi = \varphi_1, \ldots, \varphi_p \in \mathrm{Irr}(K_u)$ are the distinct conjugates of φ in G. Hence if we consider $T := \mathrm{I}_G(\varphi)$ then $K_u \leqslant T < G$ and $|G : T| = p$, so there exists $\psi \in \mathrm{Irr}(T)$ such that $\psi_{K_u} = \varphi$ and $\psi^G = \chi$. Now if $\mathcal{R}$ is a representation of T affording ψ then $\mathcal{R}^G$ is a representation of G affording χ.

Case III. All $t_i = 1$ and $e_1 = 1$.

If for some $j \geqslant 1$, $e_j = 1$ and $e_{j+1} > 1$ then $\chi_{G^{(j)}}$ is an irreducible character of $G^{(j)}$. Let $\mathcal{R}$ be a representation affording $\chi_{G^{(j)}}$ for $G^{(j)}$. Then Theorem 2.1 shows how to construct an extension of $\mathcal{R}$ to G which is a representation of G affording χ.

If all $e_i = 1$ then put $H := G^{(\infty)}$. If G is solvable then $H = 1$ and this will never happen except in the trivial case when $\chi(1) = 1$. If G is not solvable then χ_H is an irreducible character of $H \neq 1$. Since H is perfect, we have to deal with the irreducible characters of perfect groups.

3. Decomposition of perfect groups

In Section 2 we have seen how we can recursively reduce our problem to the case where G is perfect. We now turn to construction of representations of perfect groups. We classify the class of perfect groups G into two subclasses depending on whether the socle $\mathrm{Soc}(G/Z(G))$ is abelian or non-abelian. We introduce the tensor product method and explain how this method enables us to reduce the problem of constructing representations of perfect groups to the case where G is a simple cover.

3.1. Tensor product

Suppose $G = HK$ is the central product of groups H and K. This means that H and K are normal subgroups of G and $[H, K] = 1$, so $H \cap K \leqslant Z(G)$. Suppose χ is an irreducible character of G and $\mathcal{R}$ is a representation of G affording χ. Then a representation of G affording χ can be constructed from representations of H and K using tensor products.

Theorem 3.1. *Suppose $G = HK$ is the central product of groups H and K. Let $\chi \in \mathrm{Irr}(G)$. Then $\chi_H = \psi(1)\phi$ and $\chi_K = \phi(1)\psi$ for some $\phi \in \mathrm{Irr}(H)$ and $\psi \in \mathrm{Irr}(K)$. Furthermore if $\mathcal{S}$ and $\mathcal{T}$ are representations of H and K affording ϕ and ψ, respectively, then $xy \longmapsto \mathcal{S}(x) \otimes \mathcal{T}(y)$ is a representation of G affording χ.*

Proof (*Compare with Curtis and Reiner (1962, Corollary 51.13)*). Define $f : H \times K \longrightarrow G$ by $f(x, y) = xy$ for $x \in H$ and $y \in K$. Since $[H, K] = 1$, f is a homomorphism onto G. By Isaacs (1976, Lemma 2.22) each element of $\mathrm{Irr}(G)$ corresponds to an element of $\mathrm{Irr}(H \times K)$. Suppose $\hat{\chi} \in \mathrm{Irr}(H \times K)$ corresponds to χ. Then by Isaacs (1976, Theorem 4.21) there exist irreducible characters $\phi \in \mathrm{Irr}(H)$ and $\psi \in \mathrm{Irr}(K)$ such that

$$\chi(hk) = \hat{\chi}((h, k)) = \phi(h)\psi(k) \qquad \text{for all } h \in H, \ \ k \in K.$$

Since $(h, 1) \in H \times K$ for each $h \in H$, $\chi(h) = \hat{\chi}(h, 1) = \phi(h)\psi(1)$, and this means $\chi_H = \psi(1)\phi$. Similarly we have $\chi_K = \phi(1)\psi$.

Suppose $\mathcal{S}$ and $\mathcal{T}$ are representations of H and K affording ϕ and ψ, respectively. We show that if $x, x' \in H$ and $y, y' \in K$ then $xy = x'y'$ implies $\mathcal{S}(x) \otimes \mathcal{T}(y) = \mathcal{S}(x') \otimes \mathcal{T}(y')$. Indeed since $xy = x'y'$ and $[H, K] = 1$, $z := x^{-1}x' = y(y')^{-1} \in H \cap K$. On the other hand $H \cap K \leqslant Z(G)$. Thus by Isaacs (1976, Lemma 2.27) there exist linear characters λ and μ on $H \cap K$ such that $\mathcal{S}(z) = \mathcal{S}(1)\lambda(z)$ and $\mathcal{T}(z) = \mathcal{T}(1)\mu(z)$ for all $z \in H \cap K$. Since $z \in H \cap K$,

$$\begin{aligned}\chi(z) &= \psi(1)\phi(z) = \psi(1)\phi(1)\lambda(z)\\ &= \phi(1)\psi(z) = \phi(1)\psi(1)\mu(z)\end{aligned}$$

and we conclude that $\lambda = \mu$. Thus

$$\begin{aligned}\mathcal{S}(x') \otimes \mathcal{T}(y') &= \mathcal{S}(xz) \otimes \mathcal{T}(yz^{-1})\\ &= \mathcal{S}(x)\lambda(z) \otimes \mathcal{T}(y)\mu(z^{-1})\\ &= \mathcal{S}(x) \otimes \mathcal{T}(y)\end{aligned}$$

as required. This shows that $xy \longmapsto \mathcal{S}(x) \otimes \mathcal{T}(y)$ is well defined, and then it is easily seen that this is a representation of G.

Finally let $h \in H$ and $k \in K$. Then

$$\mathrm{tr}(\mathcal{S}(h) \otimes \mathcal{T}(k)) = \mathrm{tr}(\mathcal{S}(h))\mathrm{tr}(\mathcal{T}(k)) = \phi(h)\psi(k) = \hat{\chi}((h, k)) = \chi(hk).$$

This implies that $hk \longmapsto \mathcal{S}(h) \otimes \mathcal{T}(k)$ is a representation of G affording χ. $\square$

3.2. Perfect groups with $\mathrm{Soc}(G/Z(G))$ non-abelian

Lemma 3.2. *If H is a perfect subgroup of a group G and K is normal in G such that G/K is solvable then $H \leqslant K$.*

Proof. Since $H/(H \cap K) \cong HK/K \leqslant G/K$, $H/(H \cap K)$ is solvable. But H is perfect, so $H/(H \cap K) = 1$, and this implies $H \leqslant K$. $\square$

Lemma 3.3. *Let $T_1, T_2, \ldots, T_k$ be k non-abelian simple groups and S_k the symmetric group of degree k. Then there exists a homomorphism*

$$\sigma : \mathrm{Aut}(T_1 \times T_2 \times \cdots \times T_k) \to S_k$$

with $\ker(\sigma) = \prod_{i=1}^{k} \mathrm{Aut}(T_i)$.

Proof. Let $G := T_1 \times T_2 \times \cdots \times T_k$, $A := \mathrm{Aut}(G)$. By assumption for $1 \leqslant i \leqslant k$, the group T_i is a non-abelian simple group so it is a minimal normal subgroup of G and $T_1, T_2, \ldots, T_k$ are the only minimal normal subgroups of G. Hence if we consider $\Omega = \{T_1, T_2, \ldots, T_k\}$ then A acts on Ω by mapping each minimal normal subgroup of G to a minimal normal subgroup of G. Therefore for each $\psi \in A$ there exist a permutation $\pi \in S_k$ such that $\psi(T_i) \cong T_{\pi(i)}$ for $1 \leqslant i \leqslant k$, where the mapping

$$\psi \overset{\sigma}{\mapsto} \pi$$

defines a homomorphism from A to S_k.

Now consider $\psi \in \ker(\sigma)$. Then $\psi(T_i) = T_i$ and

$$\psi_{|T_i} : T_i \to T_i$$

is an automorphism of T_i for each i, so $\psi_{|T_i} \in \mathrm{Aut}(T_i)$. Hence $\psi \in \prod_{i=1}^{k} \mathrm{Aut}(T_i)$. Conversely each $\psi \in \prod_{i=1}^{k} \mathrm{Aut}(T_i)$ is an automorphism of G which maps each T_i into itself. Thus $\ker(\sigma) = \prod_{i=1}^{k} \mathrm{Aut}(T_i)$. $\square$

According to the lemma above if $A = \mathrm{Aut}(T_1 \times T_2 \times \cdots \times T_k)$ and $A^* = \prod_{i=1}^{k} \mathrm{Aut}(T_i)$ then A/A^* is isomorphic to a subgroup of S_k.

Let $Z = Z(G)$ be the centre of the group G. For each subgroup H of G which contains Z denote H/Z by $\bar{H}$.

Theorem 3.4. *Let G be a finite perfect group and $\bar{S} = \mathrm{Soc}(\bar{G}) = \bar{T}_0 \times \bar{T}_1 \times \cdots \times \bar{T}_n$ where $\bar{T}_0$ is the abelian part of $\bar{S}$ and for $1 \leqslant i \leqslant n$, $\bar{T}_i$ are non-abelian simple groups. Let $\bar{S}^* = \bar{T}_1 \times \bar{T}_2 \times \cdots \times \bar{T}_n$ and $\bar{C} = C_{\bar{G}}(\bar{S}^*)$. If $n \leqslant 4$, then $\bar{G} = \bar{C} \times \bar{S}^*$ and G is the central product of $C, T_1, T_2, \ldots, T_n$. In particular if $\bar{T}_0 = 1$ then $\bar{C} = 1$ and so G is the central product of $T_1, T_2, \ldots, T_n$.*

Proof. By assumption, $\bar{C} = C_{\bar{G}}(\bar{S}^*)$ so $\bar{S}^* \lhd \bar{G}$ implies $\bar{C} \lhd \bar{G}$ and $\bar{C} \cap \bar{S}^* = 1$ since $Z(\bar{S}^*) = 1$. Since $\bar{G}$ acts by conjugation on $\bar{S}^*$, we define a homomorphism

$$\phi : \bar{G} \longrightarrow \mathrm{Aut}(\bar{S}^*)$$

with $\ker(\phi) = \bar{C}$ and $\bar{G}/\bar{C}$ isomorphic to a subgroup $B = \phi(\bar{G})$ of $A := \mathrm{Aut}(\bar{S}^*)$. On the other hand

$$A^* = \mathrm{Aut}(\bar{T}_1) \times \mathrm{Aut}(\bar{T}_2) \times \cdots \times \mathrm{Aut}(\bar{T}_n) \lhd A.$$

Since $n \leqslant 4$ Lemma 3.3 shows we can embed A/A^* in S_4.

Since $\bar{C} \cap \bar{S}^* = 1$, the restriction of ϕ on $\bar{S}^*$ is one to one and this means $\bar{S}^* \cong \phi(\bar{S}^*)$. Since $\bar{T}_i$ are non-abelian simple for $i \neq 0$, $Z(\bar{T}_i) = 1$ and thus

$$\bar{S}^* \cong \mathrm{Inn}(\bar{T}_1) \times \mathrm{Inn}(\bar{T}_2) \times \cdots \times \mathrm{Inn}(\bar{T}_n) = \mathrm{Inn}(\bar{S}^*) = \phi(\bar{S}^*) = I^*, \text{ say.}$$

Now by "Schreier's Conjecture" the group of outer automorphisms of each finite simple group is solvable (the proof uses the classification of finite simple groups). Thus $\mathrm{Out}(\bar{T}_i) = \mathrm{Aut}(\bar{T}_i)/\mathrm{Inn}(\bar{T}_i)$ is solvable for $i > 0$ and so

$$A^*/I^* \cong \mathrm{Out}(\bar{T}_1) \times \mathrm{Out}(\bar{T}_2) \times \cdots \times \mathrm{Out}(\bar{T}_n) = O^*$$

is solvable.

Since A/A^* is isomorphic to a subgroup of S_4, it is solvable. On the other hand B is a perfect subgroup of A, so by Lemma 3.2 we have that B is a perfect subgroup of A^*. I^* is a normal subgroup of A^* and $A^*/I^* \cong O^*$ is solvable; thus by Lemma 3.2 we get that B is isomorphic to a subgroup of I^*. However we have $\bar{S}^* \cong I^*$ embedded in B. Hence $\bar{S}^* \cong B \cong \bar{G}/\bar{C}$. Since $\bar{C} \cap \bar{S}^* = 1$, this implies $\bar{G} \cong \bar{C} \times \bar{S}^*$ which is $\bar{G} \cong \bar{C} \times \bar{T}_1 \times \bar{T}_2 \times \cdots \times \bar{T}_n$. Now we show that G is a central product of $C, T_1, T_2, \ldots, T_n$. Suppose U equals C or some T_i and V is the product of the remaining factors. This means if $U = C$ then $V = T_1 \times \cdots \times T_n$ and if $U = T_i$ for some $1 \leqslant i \leqslant n$ then $V = C \times T_1 \times \cdots \times T_{i-1} \times T_{i+1} \times \cdots \times T_n$. We show that $[U, V] = 1$. Let $u \in U$ and consider the mapping $f_u : V \longrightarrow Z(G)$ defined by $f_u(y) = [u, y]$. Since $[u, y] \in Z(G)$,

$$\begin{aligned} f_u(yy') = [u, yy'] &= u^{-1}(y')^{-1}y^{-1}uyy' = u^{-1}(y')^{-1}uu^{-1}y^{-1}uyu^{-1}uy' \\ &= [u, y]u^{-1}(y')^{-1}uu^{-1}uy' = [u, y][u, y'] = f_u(y) f_u(y') \end{aligned}$$

shows f_u is a homomorphism. Since $\mathrm{Im}(f_u) \leqslant Z(G)$ is abelian, $\ker(f_u)$ contains V'. Since G is perfect, $V = V'$ and so $\ker(f_u) = V$. Thus $[u, y] = 1$ for all $y \in V$. Therefore $[U, V] = 1$ and G is a central product of U and V. Now the general result follows by induction on the number of factors in G.

If $\bar{T}_0 = 1$ and $\bar{C} \neq 1$ then $\bar{C}$ contains a minimal normal subgroup of $\bar{G}$ and we get $\bar{C} \cap \bar{S}^* \neq 1$ which contradicts $Z(\bar{S}^*) = 1$. Therefore $\bar{C} = 1$ and G is a central product of $T_1, T_2, \ldots, T_n$. □

The relevance of this theorem to our problem is the following corollary.

Corollary 3.5. *Let G be a group satisfying the conditions of the theorem above and suppose that G has a faithful character of degree <32. Then G is a central product of $C, T_1, \ldots, T_n$ with $n \leqslant 4$.*

Proof. Under the hypotheses of Theorem 3.4, $T_1, \ldots, T_n$ are non-abelian perfect groups, so the degree of a nontrivial character of each T_i is at least 2. Therefore if $n \geqslant 5$ and χ is a faithful character of G then $\chi(1) \geqslant 2^5 = 32$ (Theorem 3.1). Thus for faithful characters of degree less than 32 we have $n \leqslant 4$ and the second part of the theorem above applies. □

Suppose G is a group satisfying the conditions of the theorem above with $n \leqslant 4$. If $\bar{G}$ has more than one factor then we can use the tensor product method to construct representations of G from representations of proper subgroups of smaller degree

(Theorem 3.1). Otherwise $\bar{S} = \bar{T}_1 = \bar{G}$ or $\bar{S} = \bar{T}_0$. In other words, $G/Z(G)$ is a non-abelian simple group or $\mathrm{Soc}(G/Z(G))$ is abelian. We consider these cases separately.

4. Perfect groups with a single component

4.1. Character restriction

Suppose χ is an irreducible character of a finite group G. One method of constructing a representation of G affording χ has been presented in Dixon (1993). This is applicable whenever G has a subgroup H such that χ_H has a linear constituent with multiplicity 1. We call such a subgroup H a χ-subgroup and will refer to this method as the character restriction method. In general there is no method for locating χ-subgroups, but in many cases when the method described in Dixon (1993) is applicable, we have found that some p-subgroup is a χ-subgroup (see Dabbaghian-Abdoly, 2003). Practically it is more difficult to find a character subgroup for characters of higher degrees.

Following Dixon (1993) the character restriction method can be described briefly as follows.

Suppose H is a χ-subgroup and that θ is a constituent of degree 1 and multiplicity 1 in χ_H. Define

$$\alpha(t) := \sum_{z \in H} \theta(z^{-1})\chi(zt^{-1}) \qquad \text{for all} \qquad t \in G.$$

Then $A = [\alpha(yx^{-1})]_{x,y \in G}$ is a $|G| \times |G|$ hermitian matrix of rank $d := \chi(1)$. It is possible to choose d elements $x_1, \ldots, x_d \in G$ such that the $d \times d$ submatrix $[\alpha(x_j x_i^{-1})]$ is nonsingular. Define $A(x)$ to be the $d \times d$ matrix $[\alpha(x_j x^{-1} x_i^{-1})]$ for each $x \in G$. Then the mapping $x \longmapsto A(x).A(1)^{-1}$ is a representation of G which affords χ. See Dixon (1993) for proof (note that in several places x_i^{-1} is incorrectly written as x_i).

4.2. *Perfect groups with* $\mathrm{Soc}(G/Z(G))$ *non-abelian simple*

One of the main problems in using the character restriction method is finding a suitable χ-subgroup (indeed, it is known that for some characters no such χ-subgroups exist). In our algorithm the method will only be applied to perfect groups of two special types: (i) simple groups and their covers; and (ii) some exceptional perfect groups G with abelian $\mathrm{Soc}(G/Z(G))$.

The author has shown in his thesis (Dabbaghian-Abdoly, 2003, Section 4) that, for every group G which is a simple group or its central cover, and every $\chi \in \mathrm{Irr}(G)$ of degree <32, G has a χ-subgroup. In most cases this χ-subgroup is a Sylow p-group (often a p-subgroup). Exceptions occur for certain characters for the groups $3.\mathrm{O}_7(3)$, $3.\mathrm{U}_6(2)$ and the covering groups of $\mathrm{U}_4(3)$. See Dabbaghian-Abdoly (2003) for details.

Hence using the character restriction method we can compute representations of degree <32 of finite simple groups and their covers.

4.3. *Perfect groups with* Soc$(G/Z(G))$ *abelian*

Suppose G is a perfect group with Soc$(G/Z(G))$ abelian and χ is a faithful irreducible character of G. If there exists an abelian normal subgroup A of G such that $A \nleqslant Z(G)$ then using Clifford's Theorem

$$\chi_A = e\sum_{i=1}^{t}\phi_i$$

where $\phi = \phi_1, \ldots, \phi_t$ are distinct irreducible characters of A of degree 1 conjugate to ϕ in G. Since $A \nleqslant Z(G)$, $t > 1$ and we can use the induction method.

Thus suppose $Z(G)$ is the maximal normal abelian subgroup of G. The following theorem is due to Isaacs (1975).

Theorem 4.1 (*Short, 1992, page 31*). *Let G be a group with centre $Z := Z(G)$ and H be a subgroup of G such that*

(1) $Z(H) = Z$,
(2) $[H, G] \leqslant Z$, *and*
(3) $|\mathrm{Hom}(H/Z, Z)| \leqslant |H/Z|$.

Then $G/Z = H/Z \times C_G(H)/Z$.

We will also need:

Theorem 4.2 (*Dixon, 1971, Theorem 4.4*). *Let χ be a faithful irreducible character of degree n of a group G and suppose $Z := Z(G)$ is the unique maximal normal abelian subgroup of G. Let $F :=$ Fit(G) be the Fitting subgroup of G. Then:*

1. *F/Z is the unique maximal normal abelian subgroup of G/Z.*
2. *$|F : Z| = d^2$ for some divisor d of n and in particular $d = n$ if χ_F is irreducible.*
3. *The Sylow subgroups of F/Z are elementary abelian.*
4. *Let $d = p_1^{l_1} \ldots p_s^{l_s}$ be the prime decomposition of d. Then there exists a homomorphism θ of G into $\prod_{i=1}^{s} \mathrm{Sp}(2l_i, p_i)$ with*

$$\ker(\theta) = \{g \in G \mid [g, x] \in Z \text{ for all } x \in F\} = C_G(F/Z).$$

Suppose G is a finite group, $Z(G)$ is the maximal normal abelian subgroup and Soc$(G/Z(G)) = T_0/Z(G)$ is abelian. We shall show that in this case the Fit$(G) = C_G(\mathrm{Fit}(G)/Z(G))$ by proving the following lemma, which is a generalization of Dixon (1971, Theorem 4.5).

Lemma 4.3. *Let G be an irreducible subgroup of $GL(V)$ where V is a vector space over $\mathbb{C}$ and let $Z(G)$ be the maximal normal abelian subgroup of G. Suppose* Soc$(G/Z(G))$ *is abelian. Then $C_G(\mathrm{Fit}(G)/Z(G)) = \mathrm{Fit}(G)$.*

Proof. Define $Z := Z(G)$, $F := \mathrm{Fit}(G)$ and $C := C_G(F/Z)$. Then by Theorem 4.2, F/Z is abelian and we get $F \leqslant C$. Now we check the conditions of Theorem 4.1 for the group C and subgroup F. Since Z is the maximal normal abelian subgroup of G and $Z(F)$ is a characteristic subgroup of F, $Z(F) \subseteq Z$ and $Z(C) \subseteq Z$. Since $Z \subseteq C$ therefore

$Z \subseteq Z(C)$, and since $Z \subseteq F$, $Z \subseteq Z(F)$. Hence $Z(F) = Z(C) = Z$. This proves condition (1) of Theorem 4.1. For (2) the definition of C shows $[F, C] \leqslant Z(C)$. Finally since Z is a group of scalars, Z is isomorphic to a subgroup of $\mathbb{C}^*$ and this means each homomorphism from F/Z to Z is a representation of degree one. By Theorem 4.2, F/Z is abelian so there are exactly $|F/Z|$ representations of degree 1 for F/Z which implies condition (3). Therefore by Theorem 4.1, $C/Z = F/Z \times C_C(F)/Z$.

Finally we show $C_C(F)/Z = 1$. If $C_C(F)/Z \neq 1$ then G/Z has a minimal normal subgroup contained in $C_C(F)/Z$. Since $C_G(F)/Z \cap F/Z = 1$ and $\mathrm{Soc}(G/Z) \subseteq F/Z$, by hypothesis we have a contradiction. Hence $C_C(F)/Z = 1$ and so $F/Z = C/Z$ and therefore $F = C$. □

Theorem 4.4. *Let G be a group such that $Z(G)$ is the unique maximal normal abelian subgroup of G and suppose $\mathrm{Soc}(G/Z(G))$ is abelian. If χ is a faithful irreducible character of G of degree n then $|\mathrm{Fit}(G) : Z(G)| = d^2$ for some divisor $d = p_1^{l_1} \ldots p_s^{l_s}$ of n and the factor group $G/\mathrm{Fit}(G)$ is isomorphic to a subgroup of $\prod_{i=1}^{s} \mathrm{Sp}(2l_i, p_i)$.*

Proof. This follows at once from Theorem 4.2 and Lemma 4.3. □

Put $F := \mathrm{Fit}(G)$. If χ_F contains at least two distinct irreducible constituents, then χ is imprimitive and we can reduce our problem to construction of a representation for a proper subgroup of G. Thus we consider the case where $\chi_F = e\theta$ for some $e \geqslant 1$ and $\theta \in \mathrm{Irr}(F)$. In this case θ is G-invariant (i.e., $\mathrm{I}_G(\theta) = G$).

If $e = 1$ then χ_F is an irreducible character of F, so Theorem 2.1 shows how we can extend a representation of F affording χ_F to a representation of G affording χ and we have reduced the problem to a smaller group.

Now consider the case where $e > 1$. We consider the different possible values of e and $\theta(1)$. First of all we show that $\theta(1) > 1$. If $\theta(1) = 1$ then the elements of F are scalar and so $F \subseteq Z(G)$ and this means that $F/Z(G) = 1$. On the other hand $T_0/Z(T_0)$ is a homomorphic image of $\bar{T}_0$ and so is abelian. Therefore T_0 is nilpotent and this implies $T_0 \subseteq F$. Hence $\bar{T}_0 = \mathrm{Soc}(G/Z(G)) = 1$. This implies $G = Z(G)$ contracting the hypothesis that G is perfect. Thus $\theta(1) > 1$ as claimed.

Recall that if H is a subgroup of G and μ is an irreducible character of H, then μ is **extendible** to G if there exists an irreducible character ρ of G such that $\rho_H = \mu$.

Theorem 4.5 (*Gallagher*). *Suppose G is a group and χ is an irreducible character of G. Let N be a normal subgroup of G and μ be an irreducible character of N such that $\langle \chi_N, \mu \rangle \neq 0$. If μ is extendible to G with $\rho_N = \mu$ for some $\rho \in \mathrm{Irr}(G)$, then there exists $\alpha \in \mathrm{Irr}(G/N)$ such that $\chi = \alpha\rho$.*

Proof. See Isaacs (1976, Corollary 6.17). □

Thus in the case where $\chi_F = e\theta$ ($\theta \in \mathrm{Irr}(F)$ and $e > 1$) we can solve our problem if we can find $\rho \in \mathrm{Irr}(G)$ such that $\rho_F = \theta$ and $\alpha \in \mathrm{Irr}(G/F)$ such that $\chi = \alpha\rho$. The theorem below gives a condition for θ to be extendible to G.

Theorem 4.6. *Let $N \lhd G$ and let $\theta \in \mathrm{Irr}(N)$ be invariant in G. Suppose that for each prime p there is a Sylow p-subgroup P/N of G/N such that θ is extendible to P. Then θ is extendible to G.*

Proof. See Isaacs (1976, Corollary 11.31). □

By the theorem above, if we show that for each Sylow subgroup P/F of G/F the irreducible character θ of F is extendible to P, then θ is extendible to G. Then we know that there exists an irreducible character α of G with $F \subseteq \ker\alpha$ such that $\alpha(1) = e$ and $\chi = \alpha\rho$. If $\mathcal{R}$ and $\mathcal{S}$ are representations of G affording α and ρ, respectively, then $\mathrm{tr}(\mathcal{R}(x) \otimes \mathcal{S}(x)) = \mathrm{tr}(\mathcal{R}(x))\mathrm{tr}(\mathcal{S}(x)) = \alpha(x)\rho(x) = \chi(x)$. This implies that $x \longmapsto \mathcal{R}(x) \otimes \mathcal{S}(x)$ is a representation of G affording χ.

Theorem 4.7. *Suppose G is a perfect group, $Z(G)$ is a maximal normal abelian subgroup, and $\mathrm{Soc}(G/Z(G))$ is abelian. Let χ be a faithful irreducible character of G, $F := \mathrm{Fit}(G)$, and $\chi_F = e\theta$ for $\theta \in \mathrm{Irr}(F)$ and $e > 1$. If $e = p$ is a prime then either θ is extendible to G or χ_P is irreducible, where P/F is a Sylow p-subgroup of G/F.*

Proof. Suppose Q/F is a Sylow q-subgroup of G/F and $\chi_Q = \sum e_i\psi_i$ for $\psi_i \in \mathrm{Irr}(Q)$. Since θ is invariant in G, there exists integer f_i such that $(\psi_i)_F = f_i\theta$ for each i, and $\chi_F = e\theta$ implies $e = \sum e_i f_i$. By Clifford's Theorem $f_i \mid |Q : F|$, so $f_i = q^{\beta_i}$ for some $\beta_i \geqslant 0$. If $\beta_i = 0$ for some i then $f_i = 1$ and we have $(\psi_i)_F = \theta$ and θ is extendible to Q. Therefore using Theorem 4.6 we have that θ is extendible to G unless for some q we have $\beta_i > 0$ for all i.

Suppose $\beta_i > 0$ for all i. Then $q \mid f_i$ for each i and so $q \mid e$. Since $e = p$ is prime, $q = p$. Since $e = \sum e_i f_i$ we conclude that $e_1 = 1$, $f_1 = p$ and $e = e_1 f_1$. This implies $\chi_Q = \psi_1$ is an irreducible character of Q and Q/F is a Sylow p-subgroup of G/F. □

Theorem 4.8. *If χ is a faithful irreducible character of G of degree n and $G/Z(G)$ is abelian then $|G : Z(G)| = n^2$.*

Proof. See Isaacs (1976, Theorem 2.31). □

Corollary 4.9. *Suppose G is a perfect group for which $Z(G)$ is a maximal normal abelian subgroup and $F := \mathrm{Fit}(G)$. If χ is a faithful irreducible character of G such that $\chi_F = e\theta$ for $\theta \in \mathrm{Irr}(F)$, then $|F : Z(G)| = \theta(1)^2$.*

Proof. Since $Z(G)$ is the maximal normal abelian subgroup of G and $Z(F)$ is a characteristic subgroup of F, $Z(F) \subseteq Z(G)$. On the other hand $Z(G) \subseteq F$ implies $Z(G) \subseteq Z(F)$. Hence $Z(F) = Z(G)$. Now since χ is faithful for G and $\chi_F = e\theta$, θ is faithful for F. Hence the Theorem shows $|F : Z(G)| = \theta(1)^2$. □

Theorem 4.10. *Suppose G is a perfect group with $Z(G)$ a maximal normal abelian subgroup and $\mathrm{Soc}(G/Z(G))$ abelian. Put $F := \mathrm{Fit}(G)$. If χ is a faithful irreducible character of G with $\chi_F = e\theta$ for $\theta \in \mathrm{Irr}(F)$, then $\theta(1) \notin \{2, 3, 6\}$.*

Proof. If $\theta(1) = d = p_1^{l_1} \ldots p_s^{l_s}$ then Theorem 4.4 and Corollary 4.9 implies G/F is isomorphic to a subgroup of $\prod_{i=1}^{s} \mathrm{Sp}(2l_i, p_i)$. Since G is perfect, G/F is perfect. If $\theta(1) = 2, 3$ or 6, G/F is isomorphic to a subgroup of $\mathrm{Sp}(2, 2), \mathrm{Sp}(2, 3)$, or $\mathrm{Sp}(2, 2) \times \mathrm{Sp}(2, 3)$, respectively. But none of these groups contains any perfect subgroup so $\theta(1) \notin \{2, 3, 6\}$. □

Theorem 4.7 shows how to deal with the case where e is a prime and Theorem 4.10 shows that the case where $\theta(1) \mid 6$ cannot occur. Thus if we restrict the degree of the character χ to less than 32 then the only remaining cases to consider are

$$(\chi(1), \theta(1), e) = (16, 4, 4), (20, 5, 4), (24, 4, 6), (28, 7, 4), (30, 5, 6).$$

The next section deals with these exceptional cases and shows that for each of these cases we can use the character restriction method to calculate a representation.

4.4. *Exceptional characters of perfect groups with* $\mathrm{Soc}(G/Z(G))$ *abelian*

Lemma 4.11. *If G is a perfect group and χ is a faithful irreducible character of degree n for G, then $|Z(G)| \mid n$.*

Proof. Let $\mathcal{R}$ be a representation of G affording χ. Since G is perfect, $\det(\mathcal{R}(x)) = 1$ for each $x \in G$. On the other hand, since χ is faithful, $Z(G)$ is cyclic (see Isaacs, 1976, Theorem 2.32). Suppose $Z(G) = \langle z \rangle$ has order m, say. Since $\mathcal{R}(z)$ is a scalar, there is an mth root of unity ω such that

$$\mathcal{R}(z) = \begin{pmatrix} \omega & & & \\ & \omega & & \\ & & \ddots & \\ & & & \omega \end{pmatrix}$$

with $\det(\mathcal{R}(z)) = \omega^n = 1$. This implies $m \mid n$. $\square$

For the cases where χ has degree 16, 20, 24, 28, and 30, using Theorem 4.4 we have that the perfect group G/F is isomorphic to a subgroup of $\mathrm{Sp}(4, 2)$, $\mathrm{Sp}(2, 5)$, $\mathrm{Sp}(4, 2)$, $\mathrm{Sp}(2, 7)$, and $\mathrm{Sp}(2, 5)$, respectively. Therefore G/F is isomorphic to A_5 or A_6, $\mathrm{PSL}(2, 5)$, A_5 or A_6, $\mathrm{PSL}(2, 7)$, and $\mathrm{PSL}(2, 5)$, respectively.

If χ has degree 20, 28, and 30 then using Holt and Plesken (1989), The GAP Group (2004), and Lemma 4.11, for each character of these degrees, there exists only one perfect group. Computations in `GAP` show that these perfect groups contain a χ-subgroup of order 50, 98, and 125, respectively.

For 16 or 24 we have more than one perfect group with characters of these degrees. But computation shows that in each case these perfect groups contain χ-subgroups containing the centre of G and having order $2^\alpha 3^\beta$ for some α and β. See Dabbaghian-Abdoly (2003) for details.

Therefore using the character restriction method, we can construct a representation of G affording χ.

5. Run-times

The results and the algorithm in this paper have been implemented in the `GAP` package `REPSN` (Dabbaghian-Abdoly, 2004) as the function `IrreducibleAffordingRepresentation`. Finding a theoretical bound on the cost of the algorithm is a difficult task, since it frequently uses high level subroutines, which, in the actual implementation, are provided by `GAP`. The cost of these subroutines is usually not provided in the

Table 1
Examples of the REPSN run-time behaviour

Group	Order	$\chi(1)$	T_{Ind}	T_{Ext}	T_{Chr}	T	T_M	T^*
G_1	2744	14	0.06	0.82	0	84.78	174.45	Failed
G_2	373248	32	0.04	0	0	250.16	250.16	880.61
G_3	10368000	30	0.13	0	20.85	258.1	258.1	2744.4
G_4	14400	25	0	0.4	2.359	19.53	85.9	112.14
G_5	95040	16	0	0	18.1	18.23	18.23	24.36
G_6	1920	8	0	1.95	0	3.58	2.6	29.13
G_7	15000	10	0.02	24.5	0	43.5	52.44	53.17
G_8	115248	42	0.11	0.55	1.98	13.94	69.61	42065.95
G_9	360000	25	0.23	0	1.36	24.53	24.53	1390.86

GAP manual. For this reason we restrict ourselves to providing some examples (Table 1) that illustrate the algorithm run-time behaviour.

The only previous program in GAP for computing representations of general groups was IrreducibleRepresentationsDixon which was based on the algorithm described in Dixon (1993). The program was not satisfactory, in part because it needed a long time to search for χ-subgroups, and in part because the method is not always applicable, so the program would often fail. For example, if G is the semidirect product of a Sylow 7-subgroup of $\mathrm{SL}(3, 7)$ and the quaternion group of order 8, then G is solvable and an irreducible character χ of degree 14 of G has no χ-subgroups. This group is introduced by G. Glauberman in Janusz (1966).

In the following table we give the time spent by GAP for constructing representations of nine different groups affording an irreducible character χ of degree $\chi(1)$. These groups are sorted according to the methods explained in this paper.

The group G_1 is the Glauberman's example explained above. This is a solvable group of the form $P \rtimes Q_8$, where P is a Sylow 7-subgroup of $\mathrm{SL}(3, 7)$. A representation of G_1 of degree 14 is constructed by extending a representation of degree 7 of a subgroup of G_1 and then inducing to a representation of degree 14 of G_1. The group G_2 is solvable; its derived series has length 7. The rest are nonsolvable groups. The group G_3 is a nonsolvable primitive permutation group of degree 125 such that $G_3^{(4)}$ is perfect and is isomorphic to the direct product of three copies of A_5. The group G_4 is a primitive permutation group of degree 25 of the form $(A_5 \times A_5):2^2$ with $A_5 \times A_5$ as its derived subgroup. A representation of G_4 of degree 25 was constructed by first computing a representation of degree 25 of $A_5 \times A_5$ as a tensor product of two representations of degree 5 and then extending to a representation of degree 25 of G_4. The group G_5 is the Mathieu simple group M_{12} as a permutation group of degree 12. The groups G_6 to G_9 are perfect groups. These groups are available in the GAP library of perfect groups. We use the notation in Holt and Plesken (1989) to describe the structure of these groups. The group G_6 is a perfect permutation group of degree 32 of the form $A_5\ 2^{4'}\mathbf{C}\ 2^1$ with abelian $\mathrm{Soc}(G_6/Z(G_6))$. If F is the Fitting subgroup of G_6, then G_6 contains a subgroup P such that P/F is a Sylow 2-subgroup of G_6/F and the restriction of χ on P is irreducible. The group G_7 is a perfect permutation group of degree 125 of the form $A_5\ 2^1\ 5^2\ \mathbf{C}\ 5^1$. A representation of

G_7 of degree 10 is computed by using the extension method (Section 2.2) twice: first for extending a representation of degree 5 to a representation of a subgroup of G_7 and then for extending a representation of degree 10 to a representation of G_7. The group G_8 is also a perfect permutation group of degree 343 of the form $\mathrm{PSL}_3(2)\ 2^1\ 7^2\ \mathbf{C}\ 7^1$. REPSN constructs a representation of G_8 of degree 42 by inducing a representation of degree 7. This is an example which shows that, in some cases, REPSN is more than 1000 times faster than the former program in GAP. Finally G_9 is a perfect permutation group of degree 49 of the form $(A_5 \times A_5)\ 2^2\ \#\ 5^2$. A representation of G_9 of degree 25 is found by computing a tensor product of two representations of degree 5 of subgroups isomorphic to A_5.

In the following table $\mathrm{T}_{\mathrm{Ind}}$, $\mathrm{T}_{\mathrm{Ext}}$ and $\mathrm{T}_{\mathrm{Chr}}$ are times spent for induction (Section 2.1), extension (Section 2.2), and character restriction methods (Section 4.1), respectively. Also T, T_M, and T^* are execution times for the REPSN program, the REPSN program using Minkwitz's method for extending a representation, and the formerly available program in GAP, respectively. The numbers in this table are the cpu times (processor times) in seconds (the machine used was a Pentium IV, 2.9 GHz).

The times given in the table show that most of the time taken in executing our program is spent in standard GAP procedures such as computing normal chains, finding generators for subgroups, and calculating with characters. The effectiveness of our program owes a lot to the efficiency of these procedures.

Acknowledgments

The results of this paper were obtained during my Ph.D. studies at Carleton University and are also contained in my thesis (Dabbaghian-Abdoly, 2003) with the same title. I would like to express deep gratitude to my supervisor Professor John D. Dixon whose guidance and support were crucial for the successful completion of this project.

References

Babai, L., Rónyai, L., 1990. Computing irreducible representations of finite groups. Math. Comp. 55, 705–722.

Babai, L., Friedl, K., 1991. Approximate representation theory of finite groups. Proc. Found. Comp. Sci. 733–742.

Baum, U., 1991. Existence and efficient construction of fast Fourier transforms on supersolvable groups. Comput. Complexity 1, 235–256.

Baum, U., Clausen, M., 1995. Computing irreducible representations of supersolvable groups. Math. Comp. 63, 351–359.

Blichfeldt, H.F., 1917. The Finite, Discontinuous Primitive Groups of Collineations in Four Variables. Chicago University Press.

Böge, S., 1993. Realisierung $p-1$-dimensionaler Darstellungen von $\mathrm{PSL}(2, p)$. Arch. Math. 60, 121–127.

Brauer, R., 1967. Über endliche lineare Gruppen von Primzahlgrad. Math. Ann. 169, 73–96.

Brott, C., Neubüser, J., 1970. A programme for the calculation of characters and representations of finite groups. In: Leeds, J. (Ed.), Conference on Computational Problems in Abstract Algebra. Pergamon Press, Oxford.

Burnside, W., 1955. Theory of Groups of Finite Order, 2nd ed. 1911. Reprinted by Dover, New York.

Cooperman, G., Finkelstein, L., 1993. Combinatorial tools for computational group theory. In: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11. Amer. Math. Soc., Providence, RI, pp. 53–86.

Curtis, C.W., Reiner, I., 1962. Representation Theory of Finite Groups and Associative Algebras. Wiley (Interscience), New York.

Dabbaghian-Abdoly, V., 2003. An algorithm to construct representations of finite groups. Ph.D. Thesis, School of Mathematics, Carleton University.

Dabbaghian-Abdoly, V., 2004. RPSEN—A Package for Constructing Representations of Finite Groups. GAP Package. http://www.gap-system.org/Packages/repsn.html.

Dixon, J.D., 1970. Computing irreducible representations of groups. Math. Comp. 24, 707–712.

Dixon, J.D., 1971. The Structure of Linear Groups. Van Nostrand.

Dixon, J.D., 1993. Constructing representations of finite groups. In: DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11. Amer. Math. Soc., Providence, RI, pp. 105–112.

Dixon, J.D., Gollan, H., 1993. Computing primitive linear groups of small order (unpublished).

Dixon, J.D., Zalesskii, A.E., 1998. Finite primitive linear groups of prime degree. J. London Math. Soc. 2, 126–134.

Eberly, W., 1989. Computations for algebras and group representations. Ph.D. Thesis, Dept. Computer Science, Univ. Toronto.

Flodmark, S., Blokker, E., 1967. A computer program for calculation of irreducible representations of finite groups. Int. J. Quantum Chem. I S, 703–711.

The GAP Group, 2004. GAP—Groups, Algorithms, and Programming. Version 4.4. http://www.gap-system.org.

Gollan, H., Grabmeier, J., 1990. Algorithms in representation theory and their realization in the computer algebra system SCRATCHPAD. Bayreuth. Math. Schr. 33, 1–23.

Holt, D.F., Plesken, W., 1989. Perfect Groups. Clarendon Press, Oxford.

Holt, D.F., Rees, S., 1994. Testing modules for irreducibility. J. Aust. Math. Soc. A 57, 1–16.

Isaacs, I.M., 1975. Character degrees and the derived length of a solvable group. Canad. J. Math. 27, 146–151.

Isaacs, I.M., 1976. Character Theory of Finite Groups. Academic Press, New York. Reprinted by Dover, New York, 1994.

Janusz, G.J., 1966. Primitive idempotents in group algebras. Proc. Amer. Math. Soc. 17, 520–523.

Minkwitz, T., 1996. Extensions of irreducible representations. Appl. Algebra Engrg. Comm. Comput. 7, 391–399.

Müller, M., Clausen, M., 2001. An efficient computer program for the symbolic construction of irreducible representation of supersolvable groups. In: The 7th Spanish Meeting on Computer Algebra and Applications, EACA-2001.

Parker, R.A., 1984. The computer calculation of modular characters (The ‘Meat-axe’). In: Atkinson, M.D. (Ed.), Computational Group Theory: Proc. London Math. Soc. Symp. Academic Press, London, pp. 267–274.

Parker, R.A., 1998. An integral meataxe. In: London Math. Soc. Lecture Note Ser., vol. 249. Cambridge Univ. Press, Cambridge, pp. 215–228.

Pergler, M., 1995. Complex representations of $GL(2, q)$. C. R. Math. Rep. Acad. Sci. Canada. 17, 207–212.

Piatetski-Shapiro, I., 1983. Complex representations of $GL(2, K)$ for a finite field K. In: Contemp. Math., vol. 16. Amer. Math. Soc.

Plesken, W., Souvignier, B., 1996. Constructing rational representations of finite groups. Experiment. Math. 5, 39–47.

Plesken, W., Souvignier, B., 1997. Analysing finitely presented groups by constructing representations. J. Symbolic Comput. 24, 335–350.

Plesken, W., Souvignier, B., 1998. Constructing representations of finite groups and applications to finitely presented groups. J. Algebra 202, 690–703.

Short, M.W., 1992. The Primitive Soluble Permutation Groups of Degree Less than 256. In: Lecture Notes in Mathematics, vol. 1519. Springer, New York.

Wales, D.B., 1969. Finite linear groups of degree seven. I. Canad. J. Math. 21, 1042–1056.

Wales, D.B., 1970. Finite linear groups of degree seven. II. Pacific J. Math. 34, 207–235.